

Closed Systems of Invertible Maps

TIM BOYKETT^{1*†}

*Institute for Algebra, Johannes Kepler University Linz, Austria
and Time's Up Research, Linz, Austria*

We generalise clones, which are sets of functions $f : A^n \rightarrow A$, to sets of mappings $f : A^n \rightarrow A^m$. We formalise this and develop language that we can use to speak about it. We then look at bijective mappings, which have connections to reversible computation, which is important for physical (e.g. quantum computation) as well as engineering (e.g. heat dissipation) reasons. We generalise Toffoli's seminal work on reversible computation to arbitrary arity logics. In particular, we show that some restrictions he found for reversible computation on alphabets of order 2 do not apply for odd order alphabets. For A odd, we can create all invertible mappings from the Toffoli 1- and 2-gates, demonstrating that we can realise all reversible mappings from four generators. We discuss various forms of closure, corresponding to various systems of permitted manipulations. These correspond, amongst other things, to discussions about ancilla bits in quantum computation.

Key words: Toffoli gate, reversible computation, clones, multi-valued logic, general algebra, mappings, iterative algebra

1 INTRODUCTION

The goal of this paper is to generalise Toffoli's fundamental results about reversible computation. There are several motivations for an interest in reversible computation, some related to physics and engineering, others of a

* email: tim.boykett@jku.at and tim@timesup.org

† Research supported by Austrian national research agency FWF research grants P24077 and P24285.

more algebraic nature. The engineering perspective notes that destroying information creates entropy and thus heat, which is bad for circuitry and wasteful[5]. The physics perspective notes that fundamental physical processes such as inelastic collisions and quantum processes are reversible[9]. An algebraic perspective notes that we can say more about groups than about semigroups owing to the existence of inverses.

Toffoli [12, 13] introduced what later became known as the Toffoli gate, a simple yet universal basic element for computation with reversible binary logic. This paper is mostly concerned with the generalisation of this logic to multi valued logics. Our main result is the generalisation of Toffoli gates to arbitrary arities and the demonstration that the multivalued logics of odd arity are in some sense more powerful.

We use language based upon the function algebras of [10], also known as clones[11]. Mal'cev [8] introduced the concept of an iterative algebra, a generalised clone. If an iterative algebra includes the projections $\pi_i^n : (x_1, \dots, x_n) \mapsto x_i$, then it is a *clone*. In the next sections we will introduce some similar terminology to deal with arbitrary mappings, in particular bijections on A^n . Later we will see that *linear term algebras*, the reduct of iterative algebras that do not have the Δ operator, play an important role.

We introduce mappings and operations upon them, to show that there are several ways to talk about compositional closure. In particular we show that the algebra of functions has a finite signature of finitary operations (Theorem 2.10). We look at the ways that a given set of functions can generate a closed system of mappings, then at ways of embedding other mappings into these closed systems. We talk about *realising* one mapping in a multiclone generated by some other mappings.

We show that all invertible mappings on a set of odd order can be generated by four small Toffoli gates and using a definition of generation that is important from an engineering perspective, show that these are enough for all arities. We close by looking at the various forms of functional closure that arise in the discussion.

2 FUNCTION TERMINOLOGY

Given a set A , $\mathcal{O}(A) = \{f : A^n \rightarrow A | n \in \mathbb{N}\}$ is the set of all functions on A . We will use the notation of [7]. The operations of an iterative algebra are $\tau, \zeta, \Delta, \nabla, *$, defined as follows. Let f be an n -ary function, g an m -ary function. The operations τ and ζ permute variables, $(\tau f)(x_1, \dots, x_n) = f(x_2, x_1, x_3, \dots, x_n)$ and $(\zeta f)(x_1, \dots, x_n) = f(x_2, x_3, \dots, x_n, x_1)$, with

both being the identity on unary functions. The operation Δ identifies variables, so $(\Delta f)(x_1, \dots, x_{n-1}) = f(x_1, x_1, x_2, \dots, x_{n-1})$, while Δ is the identity on unary functions. The operation ∇ introduces a dummy variable, $(\nabla f)(x_0, x_1, \dots, x_n) = f(x_1, x_2, \dots, x_n)$. Lastly we have composition, so

$$(f * g)(x_1, \dots, x_{n+m-1}) = f(g(x_1, \dots, x_m), x_{m+1}, \dots, x_{n+m-1}).$$

The *full iterative algebra* is $(\mathcal{O}(A); \tau, \zeta, \Delta, \nabla, *)$ and an iterative algebra on A is a subuniverse of this. If an iterative algebra includes the projections $\pi_i^n : (x_1, \dots, x_n) \mapsto x_i$, then it is a *clone*. The *full linear term algebra* is $(\mathcal{O}(A); \tau, \zeta, \nabla, *)$ and a linear term algebra on A is a subuniverse of this.

We use S_A to denote the permutations of a set A , S_n to denote the set of bijections on $\{1, \dots, n\}$ and $S_{\mathbb{N}} = \cup_{n \in \mathbb{N}} S_n$. We multiply permutations from left to right, so $(123)(12) = (1)(23)$, thus in order to avoid difficulties, when we write permutations as functions, we introduce clarifying parentheses. Thus if $\alpha = (123)$ and $\beta = (12)$ then $(\alpha\beta)(1) = 1^{\alpha\beta} = 1$ but $\alpha \circ \beta(1) = \alpha(\beta(1)) = 3$.

Let A be a set. An (n, m) -map is a function $f : A^n \rightarrow A^m$. We call n the *arity*, m the *co-arity*. We write $M_{n,m}(A) = \{f : A^n \rightarrow A^m\}$. Then $M(A) = \bigcup_{n,m} M_{n,m}(A)$ is the set of all maps on A . A *function* is an $(n, 1)$ -map. An (n, n) -map, with arity equal to co-arity, will be called *balanced*. Furthermore, we define $B_{n,m}(A)$ as the set of all (n, m) -maps that are bijections, so for A finite $n \neq m$ implies that $B_{n,m}(A) = \emptyset$ and the bijective maps are balanced. We will write $B_n(A)$ for the balanced bijections of arity n . Similarly we write $B(A) = \bigcup_{n,m} B_{n,m}(A)$ is the set of all bijections on A , $B(A) = \bigcup_n B_n(A)$ if A is finite.

For example the map $f(x, y) = (x + y, x - y)$ on an abelian group is a balanced $(2, 2)$ -map, it is a bijection if the group is of odd order.

Definition 2.1 Let $f : A^m \rightarrow A^n$ an (m, n) -map, $\theta \in \{1, \dots, n\}^t$ without repetitions. Define $(s(\theta, f))_j = f_{\theta_j}$, the θ_j th component of f . Let $i \in \{1, \dots, m\}$ and $a \in A$. Then define

$$k(i, a, f)(x_1, \dots, x_{m-1}) = f(x_1, \dots, x_{i-1}, a, x_i, \dots, x_{m-1}).$$

We extend k to tuples. Let $\theta = \{i_1 < i_2 < \dots < i_r\} \subseteq \{1, \dots, m\}$, $\{1, \dots, m\} \setminus \theta = \{j_1 < \dots < j_{m-r}\}$. Define $k(\theta, a, f)(x_1, \dots, x_{m-r}) = f(y)$ with $y_i = a$ if $i \in \theta$, $y_{j_l} = x_l$ otherwise. Let $a_1, \dots, a_r \in A$ and define $k(\theta, (a_1, \dots, a_r), f)(x_1, \dots, x_{m-r}) = f(y)$ with $y_{i_r} = a_r$ if $i \in \theta$, $y_{j_l} = x_l$ otherwise.

We can then write $f_{\theta',\theta}^o = s(\theta, k(\theta', o, f)) = s(\theta, k(\theta', (o, \dots, o), f))$. Then $f_{\theta',\theta}^o$ has arity $m - |\theta'|$ and co-arity $|\theta|$.

For example, take the map $f(x, y) = (x+y, x-y)$ on \mathbb{Z}_7 , then $f_{(2),(1)}^5(z) = s((1), k((2), (5), f))(z) = z + 5$ is a unary function on \mathbb{Z}_n .

2.1 Operations

In this section we look at the operations that allow us to combine mappings. Our main result is that all these combinations can be written as a finite number of finitary operations.

Definition 2.2 Let $f \in M_{n,s}(A)$, $g \in M_{m,t}(A)$ be mappings.

We define $i_1 \in B_1(A)$ with $i_1(x) = x$. We write $i_n \in B_n(A)$ for the identity function on A^n .

We place two mappings next to one another to form a wider mapping.

$$\begin{aligned} f \oplus g : A^{n+m} &\rightarrow A^{s+t} \\ (x_1, \dots, x_{n+m}) &\mapsto (f_1(x_1, \dots, x_n), \dots, f_s(x_1, \dots, x_n), \\ &\quad g_1(x_{n+1}, \dots, x_{n+m}), \dots, g_t(x_{n+1}, \dots, x_{n+m})) \end{aligned}$$

We compose mappings. For $k \leq n$, $k \leq t$,

$$\begin{aligned} \circ_k(f, g) : A^{n+m-k} &\rightarrow A^{s+t-k} \\ (x_1, \dots, x_{n+m-k}) &\mapsto (f_1(g_1(x_1, \dots, x_m), \dots, g_k(x_1, \dots, x_m), x_{m+1}, \dots, x_{m+n-k}), \\ &\quad \vdots \\ &\quad f_s(g_1(x_1, \dots, x_m), \dots, g_k(x_1, \dots, x_m), x_{m+1}, \dots, x_{m+n-k}), \\ &\quad g_{k+1}(x_1, \dots, x_l), \dots, g_t(x_1, \dots, x_m)) \end{aligned}$$

For $k \geq 2$, \circ_k is a partial operation.

We identify variables.

$$\begin{aligned} \Delta f : A^{n-1} &\rightarrow A^s \\ \Delta f(x_1, \dots, x_{n-1}) &= f(x_1, x_1, \dots, x_{n-1}) \end{aligned}$$

and define $\Delta f = f$ if f has arity 1.

We introduce dummy variables.

$$\begin{aligned} \nabla f : A^{n+1} &\rightarrow A^s \\ \nabla f(x_1, \dots, x_{n+1}) &= f(x_2, \dots, x_{n+1}) \end{aligned}$$

The following operations allow us to permute the inputs and outputs of a given mapping.

$$\begin{aligned}\tau f(x_1, \dots, x_n) = (&f_1(x_2, x_1, x_3, \dots, x_n), \\ &f_2(x_2, x_1, x_3, \dots, x_n), \\ &\vdots \\ &f_s(x_2, x_1, x_3, \dots, x_n))\end{aligned}$$

$$\begin{aligned}\zeta f(x_1, \dots, x_n) = (&f_1(x_2, x_3, \dots, x_n, x_1), \\ &f_2(x_2, x_3, \dots, x_n, x_1), \\ &\vdots \\ &f_s(x_2, x_3, \dots, x_n, x_1))\end{aligned}$$

$$\begin{aligned}\bar{\tau} f(x_1, \dots, x_n) = (&f_2(x_1, x_2, x_3, \dots, x_n), \\ &f_1(x_1, x_2, x_3, \dots, x_n), \\ &\vdots \\ &f_s(x_1, x_2, x_3, \dots, x_n))\end{aligned}$$

$$\begin{aligned}\bar{\zeta} f(x_1, \dots, x_n) = (&f_2(x_1, x_2, x_3, \dots, x_n), \\ &f_3(x_1, x_2, x_3, \dots, x_n), \\ &\vdots \\ &f_s(x_1, x_2, x_3, \dots, x_n), \\ &f_1(x_1, x_2, x_3, \dots, x_n)).\end{aligned}$$

In the case that f has arity 1, $\tau f = \zeta f = f$. In the case that f has co-arity 1, $\bar{\tau} f = \bar{\zeta} f = f$.

For example, in the case that $n = t$, $f \circ_n g$ is the composition that we would expect:

$$\begin{aligned}f \circ_n g = (&f_1(g_1(x_1, \dots, x_m), \dots, g_n(x_1, \dots, x_m)), \\ &\vdots \\ &f_s(g_1(x_1, \dots, x_m), \dots, g_n(x_1, \dots, x_m)))\end{aligned}$$

Note that there are many relations amongst these operations. For instance let f have co-arity n , then $\bar{\tau}f = (\tau i_n) \circ_n f$ and $\bar{\zeta}f = (\zeta i_n) \circ_n f$. The s operator introduced above allows us to say $s((2, \dots, n+1), \nabla f) = f$.

We can look at a general form of mapping composition corresponding to clones.

Definition 2.3 *A collection of mappings on A is called a multiclone if it is closed under the operations $\{i_1, \oplus, \Delta, \nabla, \tau, \zeta\}$ and the partial operations $\{\circ_i | i \in \mathbb{N}\}$. Let $F \subseteq M(A)$ be a collection of mappings. Then we write $C_\Delta(F)$ for the closure under the operations, i.e. the multiclone generated by F .*

However in order to focus on the realm of bijective mappings, we are predominately interested in closure without the Δ and ∇ operations.

Definition 2.4 *A collection of mappings on A is called a read once multiclone if it is closed under the operations $\{i_1, \oplus, \tau, \zeta\}$ and the partial operations $\{\circ_i | i \in \mathbb{N}\}$. Let $F \subseteq M(A)$ be a collection of mappings. Then we write $C(F)$ for the closure under the operations, i.e. the read once multiclone generated by F .*

These operations reflect what [12] calls a *combinatorial network*, as well as corresponding to the idea of a read once function as used in in [3]. In particular, every output is used at most once as an input to another mapping, avoiding the duplication of variables or so-called fan-out, where one data signal is spread to two or more outputs. The mapping $\phi_n \in M_{1,n}(A)$ with $\phi_n(a) = (a, \dots, a)$ is a fan out mapping. Also, no input or output is thrown away. As a connection between these concepts, we have the following.

Lemma 2.5 *Let F be a read once multiclone. Then F is a multiclone iff $\phi_2(x) = (x, x)$, $g(x, y) = y \in F$.*

Proof: (\Rightarrow): We know that $i_2 = i_1 \oplus i_1 \in F$. We know F is a multiclone, so $\Delta i_2 \in F$. But $\Delta i_2(x_2) = (x_2, x_2) = \phi_2(x_2)$ so $\phi_2 \in F$. Similarly $\nabla i_1 = g$.

(\Leftarrow): Suppose $\phi_2 \in F$. Let $h \in F \cap M_{n,m}$ with $n \geq 2$. Then

$$\begin{aligned} (h \circ_2 \phi_2) &= h(x_1, x_1, \dots, x_{n-1}) \\ &= \Delta h(x_1, \dots, x_{n-1}) \end{aligned}$$

so F is closed under Δ .

Let $h \in F \cap M_{n,m}$. We calculate that $h \circ_1 g \in M_{n+2-1, m+1-1} = M_{n+1, m}$

$$\begin{aligned} (h \circ_1 g)(x_1, \dots, x_{n+1}) &= h(g_1(x_1, x_2), x_3, \dots, x_{n+1}) \\ &= h(x_2, \dots, x_{n+1}) \\ &= \nabla h(x_1, \dots, x_{n+1}) \end{aligned}$$

so F is also closed under ∇ , thus F is a multiclonal. \square

If we allow tuples with repetitions in the definition of $s(I, f)$, then this result shows that a read once multiclonal F will give a multiclonal $S(F)$ because $s((1, 1), i_1)$ and $s((2), i_2)$ are the two functions used in this lemma.

Definition 2.6 A read once multiclonal is called a reversible clone or revclone if each element is bijective.

Note that multiclones have the fan-out mapping by the previous Lemma, which is not surjective and thus not bijective. So no confusion can arise by the use of the phrase reversible clone rather than reversible read once multiclonal.

Note that $i_1 \oplus i_1 \oplus \dots \oplus i_1 = i_n$. We will also use \oplus to concatenate tuples, $(x_1, \dots, x_n) \oplus (y_1, \dots, y_m) = (x_1, \dots, x_n, y_1, \dots, y_m)$. Let $\alpha \in S_n$ be a permutation. Then let π_α be the function $\pi_\alpha(x_1, \dots, x_n) = (x_{\alpha^{-1}1}, \dots, x_{\alpha^{-1}n})$.

Example 2.7 The set $\{\pi_\alpha | \alpha \in S_n, n \in \mathbb{N}\}$ is a reversible clone, in fact it is the minimal reversible clone.

There exist well known reversible clones.

Example 2.8 Let A be a field. Then the collection of linear mappings on vector spaces over A form a multiclonal. The collection of invertible linear mappings $\cup_{n \in \mathbb{N}} GL(n, A)$ forms a reversible clone, but not a multiclonal. The permutation matrices form the smallest subrevclone.

Definition 2.9 Let f, g be mappings, f have arity n , g have co-arity m . Let $k = \min(m, n)$. Define $f \bullet g = f \circ_k g$.

Theorem 2.10 Let F be a collection of mappings on a set A . Then the following are equivalent:

1. F is a read once multiclonal.
2. F is closed under $\{i_1, \oplus, \tau, \zeta\} \cup \{\circ_k | k \in \mathbb{N}\}$.

3. F is closed under $\{\oplus\} \cup \{\pi_\alpha | \alpha \in S_{\mathbb{N}}\} \cup \{\circ_k | k \in \mathbb{N}\}$.

4. F is closed under $\{i_1, \oplus, \tau, \zeta, \bullet\}$.

Proof: The second case is a writing of the definition of the first. We demonstrate that the others are equivalent by showing that each collection of operations can be built from the others as terms.

$3 \Rightarrow 2$: In this signature, i_1 is π_α for α the identity permutation on $\{1\}$. \oplus is the same, as are \circ_k . Let $f \in M_{m,n}$. We see that $\tau f = f \circ_m \pi_{(1,2)}$, the permutation $(1, 2)$ acting upon $\{1, \dots, m\}$, and $\zeta f = f \circ_m \pi_{(m, \dots, 2, 1)}$, the permutation $(m, \dots, 2, 1)$ acting upon $\{1, \dots, m\}$.

$2 \Rightarrow 4$: From the definition of \bullet , we know that it can be written in terms of \circ_k for any given arguments.

$4 \Rightarrow 3$: Let α be a permutation on $\{1, \dots, n\}$. Let $\alpha = \alpha_1 \alpha_2 \dots \alpha_k$ for $\alpha_i \in \{(1, 2), (1, 2, \dots, n)\}$. Let $\beta_i = \tau$ if $\alpha_i = (1, 2)$, otherwise $\beta_i = \zeta$. Then $\pi_\alpha = \beta_k \bullet \dots \bullet \beta_1 \bullet (i_1 \oplus \dots \oplus i_1)$ with i_1 repeated n times.

Let f, g be mappings, $f \in M_{n,s}(A)$, $g \in M_{m,t}(A)$, $k \leq t$, $k \leq n$. Then we claim that

$$f \circ_k g = (f \oplus i_{m-k}) \bullet \pi_\alpha \bullet (g \oplus i_{n-k}) \quad (1)$$

with

$$\alpha = \begin{pmatrix} 1 & \dots & k & k+1 & \dots & t & t+1 & \dots & t+n-k \\ 1 & \dots & k & n+1 & \dots & t+n-k & k+1 & \dots & n \end{pmatrix}.$$

First note that because of the structure of the permutation α ,

$$(\pi_\alpha \bullet (g \oplus i_{n-k}))_j = \begin{cases} g_j(x_1, \dots, x_m) & j \leq k \\ x_{t-k+j} & k < j \leq n \\ g_{k+j-n}(x_1, \dots, x_m) & n < j \leq t+n-k \end{cases}$$

We can then calculate the right hand side of (1). For $j \leq s$, the j th entry is:

$$f_j \bullet \pi_\alpha \bullet (g \oplus i_{n-k})(x_1, \dots, x_{n+m-k}) = f_j(g_1(x_1, \dots, x_m), \dots, g_k(x_1, \dots, x_m), x_{m+1}, \dots, x_{m+n-k})$$

while for $s < j \leq s+t-k$, the j th entry is:

$$(\pi_\alpha \bullet (g \oplus i_{n-k}))_{n+j-s}(x_1, \dots, x_{n+m-k}) = g_{k+j-s}(x_1, \dots, x_m)$$

By comparing entries, we see that the left hand side and the right hand side agree at all entries and are thus equal. \square

This enables us to easily see that the operations of a read once multiclone do not destroy reversibility, so we know that $B(A)$ is the largest reversible clone on A .

Lemma 2.11 *Let $F \subseteq B(A)$. Then $C(F) \subseteq B(A)$.*

Proof: We only need to check that $B(A)$ is a read once multiclone. The operations i_1, τ, ζ are invertible. Let $f, g \in B(A)$. The inverse of $f \oplus g$ is $f^{-1} \oplus g^{-1}$. If the coarity of g is the same as the arity of f , then $(f \bullet g)^{-1} = g^{-1} \bullet f^{-1}$. If the coarity of g is less than the coarity of f , then note that $f \bullet g = f \bullet (g \oplus i_s)$ where s is the difference between the arity of f and the coarity of g . Then the coarity of $g \oplus i_s$ equals the arity of f and we are done. Similarly if the arity of f is less than the coarity of g .

Thus all of the operations of a read once multiclone map bijections to bijections, so we are done. \square

We know that there is a finite signature for read once multiclones, so we can apply the standard tools and techniques of universal algebra, such as the following.

Corollary 2.12 *Let A be a set. Then the set of read once multiclones on A , ordered by inclusion, is an algebraic lattice. The set of reversible clones on A , ordered by inclusion, is an algebraic lattice.*

Proof: The set of read once multiclones on A is the set of subuniverses of the algebra $(M(A); i_1, \oplus, \tau, \zeta, \bullet)$. These operations are all finitary, so by [2][Theorem 3.3] we have our result.

Similarly reversible clones are subuniverses of $(B(A); i_1, \oplus, \tau, \zeta, \bullet)$ and we are done. \square

We note also that the definition of a proper multiclone adds only two unary operations, so we obtain the following as a corollary to Theorem 2.10 and Corollary 2.12.

Corollary 2.13 *Let F be a collection of mappings on a set A . Then the following are equivalent:*

1. F is a multiclone.
2. F is closed under $\{i_1, \oplus, \tau, \zeta, \Delta, \nabla\} \cup \{\circ_k | k \in \mathbb{N}\}$.
3. F is closed under $\{\oplus, \Delta, \nabla\} \cup \{\pi_\alpha | \alpha \in S_{\mathbb{N}}\} \cup \{\circ_k | k \in \mathbb{N}\}$.
4. F is closed under $\{i_1, \oplus, \tau, \zeta, \Delta, \nabla, \bullet\}$.

The set of multiclones, ordered by inclusion, is an algebraic lattice.

3 REALISATION

In this section we look at the ways in which one set of mappings can be found within another.

Theorem 3.1 *Let A be a finite set. For all $g : A^m \rightarrow A^n$ there exists some integer $r = \max(m, n + \lceil \log_{|A|} \max_{a \in A^n} |g^{-1}(a)| \rceil)$, an invertible $f : A^r \rightarrow A^r$, some $o \in A$ and $\theta_1 = (1, \dots, m), \theta_2 = (1, \dots, n)$ such that $g = f_{\theta_1, \theta_2}^o$. The value of r can always be found such that $\max(m, n) \leq r \leq n + m$ and these bounds are achieved.*

Proof: Select $o \in A$ arbitrary but fixed. For each $a \in A^n$, let $x^{(1)}, \dots, x^{(k)} \in A^m$ be a lexicographical ordering of $g^{-1}(a)$. Let $b^{(1)}, \dots, b^{(k)}$ be the first k elements of A^{r-n} in lexicographical order. Define $f(x_1^{(i)}, \dots, x_m^{(i)}, o, \dots, o) = (a_1, \dots, a_n, b_1^{(i)}, \dots, b_{(r-n)}^{(i)})$ for each $i \in \{1, \dots, k\}$.

Now f is a partial injective map on A^r , thus it can be completed to a bijection of A^r .

For any $z \in A^m$, let $b = g(z_1, \dots, z_m)$. Then $(z_1, \dots, z_m) \in g^{-1}(b)$, so $f(z_1, \dots, z_m, o, \dots, o) = (b_1, \dots, b_n, c_1, \dots, c_m)$ for some $c_1, \dots, c_m \in A$.

Thus $f_{\theta_1, \theta_2}^o(z) = s(\theta_2, k(\theta_1, (o, \dots, o), f)(z)) = b = g(z)$, showing $f_{\theta_1, \theta_2}^o = g$.

The average value of $|g^{-1}(a)|$ is $\frac{|A|^m}{|A|^n} = |A|^{m-n}$. Thus we know that $\lceil \log_{|A|} \max_{a \in A^n} |g^{-1}(a)| \rceil \geq (m - n)$. This value can be minimised if all $|g^{-1}(a)|$ are equal to the average value, so $|g^{-1}(a)| = |A|^{m-n}$, so the minimum value of r is $\max(m, n)$. The maximum value is obtained if g is constant, so there is some $a \in A^n$ such that $g^{-1}(a) = A^m$. In this case, $\log_{|A|} \max_{a \in A^n} |g^{-1}(a)| = m$ and thus $r = n + m$. \square

Corollary 3.2 ([12] Theorem 4.1) *Let A be a finite set. For all $g : A^m \rightarrow A^n$ there exists $r \leq n$, invertible $f : A^{m+r} \rightarrow A^{m+r}$, $o \in A$ and $\theta_1 \in \{1, \dots, m + r\}^m, \theta_2 \in \{1, \dots, m + r\}^n$ such that $g = f_{\theta_1, \theta_2}^o$.*

Proof: Let r_0 be the value of r obtained in the theorem above. There are two possibilities for r_0 . If $r = m$ then we take $r = 0 < n$ in this theorem and we are done. If $r_0 = n + \lceil \log_{|A|} \max_{a \in A^n} |g^{-1}(a)| \rceil$ then note that $g^{-1}(a) \subseteq A^m$ so $|g^{-1}(a)| \leq |A|^m$. So $r_0 \leq n + m$ so $r \leq n$ in this theorem and we are done. \square

3.1 Forms of Realisation

We now look at several ideas about generation, corresponding to different forms of closure. While the simplest definition talks about the multicloner

generated from a set of mappings, Toffoli introduces some interesting ideas about more general, engineering inspired forms of realisation. The following is a translation of his definitions to the language we have developed here.

Definition 3.3 *Let A be a set, $F \subseteq M(A)$. Then $K(F)$ is the set of all functions we can obtain from F by inserting constants. Hence $K(F)$ the closure under all possible applications of k , including none.*

$S(F)$ is the set of all submappings of mappings in F . Then $S(F)$ is the closure under all possible applications of s .

$R(F)$ is the collection of bijections in F , i.e. $R(F) = F \cap B(A)$.

Definition 3.4 *Let F be a collection of mappings on A . A mapping $g \in M(A)$ is said to be isomorphically realised by F [12, p. 8], or realized without ancilla bits [14], if $g \in C(F)$.*

Let A be a set, $F \subseteq M(A)$ and $g \in M_{m,n}(A)$.

- *We say g is realised by F if there exists some $f \in C(F)$, $f \in M_{l,k}(A)$ and $a_1, \dots, a_{l-m} \in A$ such that for all $i \in \{1, \dots, n\}$ and for all $x_1, \dots, x_m \in A$:*

$$g_i(x_1, \dots, x_m) = f_i(x_1, \dots, x_m, a_1, \dots, a_{l-m}) \quad (2)$$

Equivalently, we can say $g \in SKC(F)$.

- *We say g is realised with no garbage if there exists some $f \in M_{l,n}(A) \cap C(F)$ satisfying (2), equivalently $g \in KC(F)$. Otherwise g is realised with garbage.*
- *We say g is realised with no constants if there exists some $f \in M_{m,k}(A) \cap C(F)$ satisfying (2), equivalently $g \in SC(F)$. Otherwise g is realised with constants.*

A mapping is isomorphically realised iff it is realised with no constants and no garbage.

This language allows us to rephrase Corollary 3.2 as:

Corollary 3.5 *For all $g \in M_{m,n}(A)$, g is realised by $B_{m+n}(A)$.*

There is a special class of realisations that have constants and garbage, but in some way do not use them up, the garbage representing the constants.

Definition 3.6 *Let A be a set, $F \subseteq M(A)$ and $g \in M_{m,n}(A)$. Then g is realised with temporary storage by F if there exists some $f \in C(F)$, $f \in$*

$M_{l,k}(A)$ and $a_1, \dots, a_{l-m} \in A$ such that $n + l - m = k$ and

$$\forall i \in \{1, \dots, n\} : g_i(x_1, \dots, x_m) = f_i(x_1, \dots, x_m, a_1, \dots, a_{l-m}) \quad (3)$$

$$\forall i \in \{1, \dots, l - m\} \forall x_1, \dots, x_m \in A :$$

$$f_{n+i}(x_1, \dots, x_m, a_1, \dots, a_{l-m}) = a_i \quad (4)$$

Definition 3.7 Let A be a set, $F \subseteq M(A)$ and $g \in M_{m,n}(A)$. Then g is realised with strong temporary storage by F if there exists some $f \in C(F)$, $f \in M_{l,k}(A)$ and $a_1, \dots, a_{l-m} \in A$ such that $n + l - m = k$ and

$$\forall i \in \{1, \dots, n\} : g_i(x_1, \dots, x_m) = f_i(x_1, \dots, x_m, a_1, \dots, a_{l-m})$$

$$\forall i \in \{1, \dots, l - m\} \forall x_1, \dots, x_m \in A :$$

$$f_{n+i}(x_1, \dots, x_m, a_1, \dots, a_{l-m}) = a_i$$

$$\forall b_1, \dots, b_m \in A : (x_1, \dots, x_{l-m}) \mapsto (f_{n+1}(b_1, \dots, b_m, x_1, \dots, x_{l-m}), \dots, \dots f_k(b_1, \dots, b_m, x_1, \dots, x_{l-m})) \in B_{l-m}(A)$$

Let $F \subseteq M(A)$ be some mappings on A . Then let $T(F)$ be the set of mappings realised with temporary storage by F , $T_S(F)$ the set of mappings realised with strong temporary storage by F .

These concepts are introduced because it allows us to use the garbage again in the next function, as we know what it looks like. Thus the extra inputs and outputs are not garbage, as they are appropriately recycled and reduce waste information. In the engineering perspective, this reduces waste heat in implementations.

Let's look at an example. Let $A = \mathbb{Z}_n$, $f(x, y) = (2x + y, xy)$. Then the map $g(x) = 2x$ is realised with temporary storage by $\{f\}$, since $g(x) = f_1(x, 0)$ and $f_2(x, 0) = 0$ for all x . However g is not realised with strong temporary storage, because $y \mapsto f_2(0, y) \notin B_1(A)$.

Lemma 3.8 Let A be finite, $F \subseteq B(A)$. Then $T_S(F) \subseteq T(F) \subseteq B(A)$.

Proof: The first inclusion is clear, as the definition of strong temporary storage is stricter than the definition of temporary storage.

Let $g \in T(F)$. This means there is some $f \in C(F)$, $a_1, \dots, a_{l-m} \in A$ satisfying the requirements (3) and (4) above. We know that $f \in B(A)$ because $F \subseteq B(A)$. Thus f is balanced, so $l = k$ and thus $n = m$. By (4), f fixes $\{(x_1, \dots, x_m, a_1, \dots, a_{l-m}) \mid x_1, \dots, x_m \in A\}$ as a set. Because f is a bijection, f is a permutation of the first m entries, so g is a permutation in $B(A)$. Thus $T(F) \subseteq B(A)$ and we are done. \square

4 THE FUNCTIONS OF A REVCLONE

In Toffoli's "Fundamental Theorem," our Corollary 3.2, he shows that all maps and thus all functions can be realised by the full reversible clone. If we look at clones, this means that the clone of all functions on A can be realised, i.e. $\mathcal{O}^A \subseteq KS(B(A))$.

Let $F \subseteq M(A)$. We call $S_1(F) = \{s((1), f) | f \in F\} = \{f_1 | f \in F\}$ the *function set* of F .

Theorem 4.1 *Let F be a read once multiclon. Then $S_1(F)$ is a linear term algebra with projections.*

Proof: The operations τ and ζ act the same in the revclone and the linear term algebra. Let $f, g \in F$, then $\nabla(f_1) = (\bar{\tau}(i_1 \oplus f))_1$. Also $f_1 * g_1 = (f \circ_1 g)_1$. Thus F being closed as a multiclon means that $S_1(F)$ is closed as a linear term algebra.

Moreover, the constants $\pi_\alpha \in F$ mean that all projections are also in $S_1(F)$, $\pi_{\alpha-1}^n = (\pi_\alpha)_1$. \square

This also applies for revclones. Note that we obtain the ∇ operation "for free" from the other operators. In general we see the following.

Corollary 4.2 *Let F be a multiclon. Then $S_1(F)$ is a clone.*

Proof: A multiclon is a read once multiclon closed under the Δ and ∇ operations on multiclones. By Theorem 4.1 we have ∇ operating on $S_1(F)$. For any $f_1 \in S_1(F)$, $\Delta(f_1) = (\Delta f)_1$ and we have clone closure. \square

This justifies the use of the expression "clone" in our expression multiclon.

Note that the mapping $F \mapsto \{f_1 | f \in F\}$ is not injective. Let $A = \{0, 1, 2, 3, 4\}$, $C = \bigcup_n GL(n, \mathbb{Z}_5) \subseteq B(A)$ a reversible clone,

$$D = \bigcup_n \{-1, 1\} SGL(n, \mathbb{Z}_5) = \{f \in C | \det f \in \{-1, 1\}\}$$

the subclone. D is a proper subrevclone of C , by the determinate. Both $GL(n, \mathbb{Z}_5)$ and $D \cap B_n(A)$ are transitive on $\mathbb{Z}_5^n \setminus \{(0, 0, 0)\}$ so both revclones have function sets that are $\bigcup_n \{f : A^n \rightarrow A | f(x_1, \dots, x_n) = \sum a_i x_i, a_i \in \mathbb{Z}_5, (a_1, \dots, a_n) \neq 0\}$, the clone of nonzero linear forms on \mathbb{Z}_5 .

Corollary 4.3 *Let F be a revclone. Then $f \in S_1(F)$, f of arity m implies that for all $a \in A$, $|f^{-1}(a)| = |A|^{(m-1)}$.*

This is a corollary of Theorem 3.1 with $n = 1$.

5 SOME RESULTS ABOUT REALISATION

Here we collect some results on reversible mappings. Much of this is based upon section 5 in [12], with the extension to Theorem 5.10.

Definition 5.1 *Let α be a permutation of A , $o \in A$ some constant, $n \in \mathbb{N}$. For $n > 1$, let*

$$TG(n, \alpha, o)(x_1, \dots, x_n)_i = x_i \quad i < n$$

$$TG(n, \alpha, o)(x_1, \dots, x_n)_n = \begin{cases} \alpha(x_n) & \text{if } x_1 = \dots = x_{n-1} = o \\ x_n & \text{otherwise} \end{cases}$$

Let $TG(1, \alpha, o)(x)_1 = \alpha(x)$. Then $TG(n, \alpha, o) \in B_n$ is an invertible mapping, the Toffoli Gate induced by n , α and o .

In [12], this mapping is defined for $A = \mathbb{Z}_2$ with α swapping 0 and 1, $o = 1$, written as $\theta^{(n)} = TG(n, (0\ 1), 1)$.

Definition 5.2 *A permutation $f \in B_n$ is elementary if there exist $x, y \in A^n$ such that $f(x) = y, f(y) = x$ and all other elements of A^n are fixed. An elementary permutation is atomic if x and y only differ in one entry, i.e. $x_i = y_i$ for all i except one.*

Lemma 5.3 *Let $n \in \mathbb{N}$, let $o \in A$. Let $f \in B_n(A)$ be atomic. Then f can be isomorphically realised by $\{TG(n, \alpha, o) | \alpha \in S_A\} \cup \{TG(1, \alpha, o) | \alpha \in S_A\}$.*

Proof: Suppose f exchanges x, y which differ at position i . Then $\pi_{(i,n)} \circ_n f \circ_n \pi_{(i,n)}$ is atomic, exchanging two vectors that differ at position n . Wlog suppose f is of this form. Let $\alpha_i := (o, x_i)$ be a transposition of A . Let $\beta_i = TG(1, \alpha_i, o)$ for $i < n$, β_n the identity. Then $\beta = \beta_1 \oplus \dots \oplus \beta_n \in B_n$ is an involution, generated by $TG(1, \alpha_i, o)$ as a revclone. Note that $\beta(x)_i = \beta(y)_i = o$ for $i < n$.

Note that $f(\beta(z)) = \beta(z)$ unless $\beta(z) = x$ respectively y . But $\beta(z) = x$ (resp. y) iff $z_i = o$ for all $i < n$ and $z_n = x_n$ (resp. y_n). So $\beta \bullet f \bullet \beta$ fixes all elements of A^n except (o, \dots, o, x_n) and (o, \dots, o, y_n) , which it exchanges. Thus $\beta \bullet f \bullet \beta = TG(n, (x_n, y_n), o)$, so f is in the revclone generated by $\{TG(n, \alpha, o) | \alpha \in S_A\} \cup \{TG(1, \alpha, o) | \alpha \in S_A\}$. \square

Theorem 5.4 ([12] Thm 5.1) *Any $f \in B_n(A)$ can be isomorphically realised by atomic permutations.*

Proof: Any permutation can be written as a product of elementary permutations. So wlog, let f be elementary, exchanging x and y .

Define a sequence $(a^{(i)} | 1 \leq i \leq n+1)$ such that for all $k \in \{1, \dots, n+1\}$, $(a^{(k)})_i = y_i$ if $i < k$, $(a^{(k)})_i = x_i$ otherwise. Then $a^{(1)} = x$, $a^{(n+1)} = y$. Note that $a^{(i)} = a^{(i+1)}$ or they differ in position i . Thus $f_i \in B_n(A)$ exchanging $a^{(i)}$ and $a^{(i+1)}$ is an atomic permutation. Now the permutation $f = f_1 \bullet f_2 \bullet \dots \bullet f_{n-1} \bullet f_n \bullet f_{n-1} \bullet \dots \bullet f_1$ is a product of atomic permutations, so we are done. \square

Corollary 5.5 *Let A be finite, say $A = \{1, \dots, k\}$. Then $B_n(A)$ is realised by $\{TG(n, \alpha, 1) | \alpha \in \{(1, 2), (1, \dots, k)\}\} \cup \{(1, 2), (1, \dots, k)\}$.*

Proof: We remind ourselves that $TG(1, \alpha, 1) = \alpha$ and thus see that the four gates listed here generate $\{TG(n, \alpha, 1) | \alpha \in S_A\} \cup \{TG(1, \alpha, 1) | \alpha \in S_A\}$. By the above Lemma, this is enough to generate all atomic permutations and thus by the above Theorem, enough to generate $B_n(A)$. \square

This is a correct form of the result hoped for in Conjecture 1 of [14]. The result that they had conjectured can be demonstrated to be false using calculations in GAP [4] for A of order 5. Interestingly enough, for A of even order, $n \geq 2$, the conjecture might hold, as calculations in GAP for small values find no contradiction. So we obtain the following conjecture that a smaller generating set might suffice.

Conjecture 5.6 *For $A = \{1, \dots, k\}$ even, $n \geq 2$,*

$$B_n(A) = C(\{(1, \dots, k), TG(n, (1, \dots, k), 1)\})$$

.

Below we will see that a small generating set exists for A of odd order.

It is worth noting that the main result in [14] is also subtly wrong for $n = 1$, as they do not have enough permutations, so the permutation $(0\ 1)$ is not generated. They have found an interesting property of ternary logic that any permutation of $\{0, 1, 2\}$ (written in \mathbb{Z}_3) can be written as $(n, n+1, n+1+1)$ or $(n, n+2, n+2+2)$, leading to their minimal generating set for $n \geq 2$.

The following results lets us calculate precisely what the n -ary part of a revclone looks like, given the generators.

Theorem 5.7 *Let $F \subseteq B(A)$, $n \in \mathbb{N}$. Let*

$$\begin{aligned} \bar{F} = & \{\bar{f} | f \in F, \text{arity } f = m < n, \bar{f} = f \oplus i_{n-m}\} \\ & \cup \{f \in F | \text{arity } f = n\} \cup \{\pi_\alpha | \alpha \in S_n\}. \end{aligned}$$

Then the group $(\langle \bar{F} \rangle; \circ_n)$ is equal to $(C(F) \cap B_n(A); \circ_n)$.

Proof: Both groups are subgroups of $(B_n(A); \circ_n)$, so we need only prove they are equal as sets.

We proceed by induction. For the case $n = 1$, \bar{F} consists of the permutations of A within F . Then the subgroup of S_A generated by these permutations is precisely $C(F) \cap B_1(A) = C(F) \cap S_A$. Then we proceed with our induction. Suppose our claim holds up to $n - 1$.

(\subseteq) : Every element $\bar{f} = f \oplus i_m$ of \bar{F} is within $C(F)$. The arity of all elements of \bar{F} is n so they are all within $B_n(A)$. So this inclusion holds.

(\supseteq) : Let $f \in C(F) \cap B_n(A)$, so f is either in \bar{F} or is a term of the form:

1. $f = g \oplus h$ for some $g, h \in C(F)$, both of smaller arity than n .
2. $f = g \circ_k h$ for some $g, h \in C(F)$, both of smaller arity than n , $k < n$.
3. $f = g \circ_k h$ for some $g, h \in C(F)$, exactly one of them in $B_n(A)$, so the other one has arity k , $k < n$.
4. $f = g \circ_n h$ for some $g, h \in C(F) \cap B_n(A)$.

In case 1, let m be the arity of g , so h has arity $n - m$. We know from our induction hypothesis that g is a product $g = \bar{g}_1 \circ_m \dots \circ_m \bar{g}_l$ of elements of the form $\bar{g}_j = f_j \oplus i_{m_j}$ for some $f_j \in F$ with arity less than m , $\bar{g}_j = f_j$ for some $f_j \in F$ with arity m , or $\bar{g}_j = \pi_{\alpha_j}$ for some permutation $\alpha_j \in S_m$. Then let $\phi_j = f_j \oplus i_{m_j+n-m} = f_j \oplus i_{m_j} \oplus i_{n-m} \in \bar{F}$ respectively $\phi_j = f_j \oplus i_{n-m} \in \bar{F}$ respectively $\phi_j = \pi_{\alpha_j} \oplus i_{n-m} = \pi_{\beta_j}$ where $\beta_j \in S_n$ is equal to α_j on $\{1, \dots, m\}$ and fixes the elements $\{m+1, \dots, n\}$. Then $\phi_1 \circ_n \dots \circ_n \phi_l = g \oplus i_{n-m}$, so $g \oplus i_{n-m} \in \langle \bar{F} \rangle$.

Similarly we can write $h \oplus i_m$ as an element of $\langle \bar{F} \rangle$. Let δ be the permutation of $\{1, \dots, n\}$ defined by

$$\delta = \begin{pmatrix} 1 & \dots & m & (m+1) & \dots & n \\ (n-m) & \dots & n & 1 & \dots & (n-m) \end{pmatrix}.$$

Then

$$\pi_{\delta^{-1}} \circ_n (h \oplus i_m) \circ_n \pi_{\delta} \circ_n (g \oplus i_{n-m}) = g \oplus h$$

Thus we see that $f \in (\langle \bar{F} \rangle; \circ_n)$.

In case 2 we proceed similarly. In this case g is m -ary and h is $n - m + k$ -ary. We use the same techniques as above to show that $g \oplus i_{n-m}, h \oplus i_{m-k} \in \langle \bar{F} \rangle$. Let δ be the permutation of $\{1, \dots, n\}$ given by

$$\delta = \begin{pmatrix} 1 & \dots & k & (k+1) & \dots & (n-m+k) & (n-m+k+1) & \dots & n \\ 1 & \dots & k & (m+1) & \dots & n & (k+1) & \dots & m \end{pmatrix}$$

so $\pi_\delta \in \bar{F}$. Then

$$\begin{aligned}
& (g \oplus i_{n-m}) \circ_n \pi_\delta \circ_n (h \oplus i_{m-k})(x_1, \dots, x_n) \\
&= (g \oplus i_{n-m}) \circ_n \pi_\delta(h_1(x_1, \dots, x_{n-m+k}), \dots, h_{n-m+k}(x_1, \dots, x_{n-m+k}), \\
&\quad x_{n-m+k+1}, \dots, x_n) \\
&= (g \oplus i_{n-m})(h_1(x_1, \dots, x_{n-m+k}), \dots, h_k(x_1, \dots, x_{n-m+k}), \\
&\quad x_{n-m+k+1}, \dots, x_n, \\
&\quad h_{k+1}(x_1, \dots, x_{n-m+k}), \dots, h_{n-m+k}(x_1, \dots, x_{n-m+k})) \\
&= (g_1(h_1(x_1, \dots, x_{n-m+k}), \dots, h_k(x_1, \dots, x_{n-m+k}), x_{n-m+k+1}, \dots, x_n), \\
&\quad \vdots \\
&\quad g_m(h_1(x_1, \dots, x_{n-m+k}), \dots, h_k(x_1, \dots, x_{n-m+k}), x_{n-m+k+1}, \dots, x_n), \\
&\quad h_{k+1}(x_1, \dots, x_{n-m+k}), \dots, h_{n-m+k}(x_1, \dots, x_{n-m+k})) \\
&= g \circ_k h(x_1, \dots, x_n)
\end{aligned}$$

Thus we see that $f \in \langle \bar{F} \rangle; \circ_n$.

In case 3 we have $k < n$ then one of the terms is of lower arity, so as above we can write $g \oplus i_{n-k}$ (respectively $h \oplus i_{n-k}$) as an element of $B_n(A)$ and have $f = (g \oplus i_{n-k}) \circ_n h$ (respectively $f = g \circ_n (h \oplus i_{n-k})$). Then we have the next case.

In case 4 we have two terms of arity n but of strictly lower term complexity. We use induction on term complexity. For the initial case, we look at the trivial terms $t \in C(F) \cap B_n(A)$. These are either elements of F or the permutations π_α for $\alpha \in S_n$. In both these cases, $t \in \bar{F}$ so $t \in \langle \bar{F} \rangle$. Now we look at $f = g \circ_n h$. Both g and h have lower term complexity than f . Thus we know that $g, h \in \langle \bar{F} \rangle$. Thus $f = g \circ_n h \in \langle \bar{F} \rangle$ and we are done. \square

We can apply this to obtain a generalisation of one of Toffoli's results.

Corollary 5.8 ([12] Thm 5.2) *Let A be of even order, $n \in \mathbb{N}$. Then $B_n(A)$ is not isomorphically realised by $\{TG(i, \alpha, o) \mid \alpha \in S_A, i < n\}$ for any $o \in A$*

Proof: For $n = 1$ the set of generators is empty, so we only have the identity permutation. For $n = 2$ and $|A| = 2$, simple calculations show that the generated revclone is of order 8, while $B_2(A)$ is of order 24.

We carry on for the other cases. Using the terminology in Theorem 5.7, we note that $\overline{TG}(i, \alpha, o) = TG(i, \alpha, o) \oplus i_{n-i}$. The action of $\tau = TG(i, \alpha, o) \oplus i_{n-i}$ on A^n , when not identity, is of the form

$$\tau(o, \dots, o, a, a_1, \dots, a_{n-i}) = (o, \dots, o, \alpha(a), a_1, \dots, a_{n-i})$$

If we write α as a product of involutions $\alpha = \alpha_1 \dots \alpha_k$ we can use the expression above to see that there will be $k|A|^{n-i}$ involutions when we write the action of τ on A^n . Thus $\overline{TG}(i, \alpha, o) = TG(i, \alpha, o) \oplus i_{n-i}$ is an even permutation in $B_n(A)$.

The action of π_β for $\beta \in S_n$ acting on A^n can also be calculated. If β is an involution in S_n , say $\beta = (ij)$, then π_β acts nontrivially on $(a_1 \dots a_i \dots a_j \dots a_n)$ with $a_i \neq a_j$. There are $\frac{|A|(|A|-1)}{2}(|A|)^{n-2}$ such tuple pairs. This number is even when $|A|$ is even (except in the case $n = |A| = 2$ which we dealt with above),

From Theorem 5.7, we know that the arity n part of $C(\{TG(i, \alpha, o) | \alpha \in S_A, i < n\})$ is generated by precisely these permutations, which are all even. Thus for some $a, b \in A$, $a \neq b$, $TG(n, (a, b), a)$ is not in the generated revclone and thus $B_n(A)$ is not isomorphically realised by $\{TG(i, \alpha, o) | \alpha \in S_A, i < n\}$. \square

The following has been noted using examples in GAP[4].

Conjecture 5.9 *Let A be of even order, $n \geq 3$. Then $\{TG(i, \alpha, o) | \alpha \in S_A, i < n, o \in A\}$ generates a subgroup of B_n isomorphic to the alternating group on A^n , except for $|A| = 2, n = 3$.*

The restriction shown in Corollary 5.8 does not hold for A odd, as we see in the following result. Moreover, it shows that we only need use the Toffoli gates of arity 1 and 2 to obtain all bijections on A .

Theorem 5.10 *Let A be of odd order. Then $B(A)$ is isomorphically realised by*

$$\{TG(i, \alpha, o) | \alpha \in S_A, i < 3\} = S_A \cup \{TG(2, \alpha, o) | \alpha \in S_A\}$$

for any $o \in A$.

Proof: Let $|A| = k$, wlog $A = \{1, \dots, k\}$, $o = 1$. We proceed by induction on n . Our start is for $n = 2$, given by the hypothesis. We assume we have shown the claim up to n . We first show that we can obtain $TG(n+1, (12), o)$ from $\{TG(i, \alpha, o) | \alpha \in S_A, i \leq n\}$. Let $\gamma = (n \ n+1)$ acting on $\{1, \dots, n+1\}$.

Define

$$\begin{aligned} \Sigma_1 = & (TG(n, (1 \dots k)^{-1}, 1) \oplus i_1) \bullet \pi_\gamma \bullet (TG(n, (12), 1) \oplus i_1) \\ & \bullet \pi_\gamma \bullet (i_{n-1} \oplus TG(2, (12), 1)) \\ & \bullet (TG(n, (1 \dots k), 1) \oplus i_1) \end{aligned}$$

We calculate.

$$\begin{aligned}
& \Sigma_1(x_1, \dots, x_{n+1}) \\
&= \begin{cases} (TG(n, (1 \dots k)^{-1}, 1) \oplus i_1) \bullet \dots \bullet (i_{n-1} \oplus TG(2, (12), 1))(x_1, \dots, x_n^{(1 \dots k)}, x_{n+1}) & \text{if } x_1 = \dots = x_{n-1} = 1 \\ (TG(n, (1 \dots k)^{-1}, 1) \oplus i_1) \bullet \dots \bullet (i_{n-1} \oplus TG(2, (12), 1))(x_1, \dots, x_n, x_{n+1}) & \text{otherwise} \end{cases} \\
&= \begin{cases} (TG(n, (1 \dots k)^{-1}, 1) \oplus i_1) \bullet \dots \bullet \pi_\gamma(x_1, \dots, x_n^{(1 \dots k)}, x_{n+1}^{(12)}) & \text{if } x_1 = \dots = x_{n-1} = 1, x_n = k \\ (TG(n, (1 \dots k)^{-1}, 1) \oplus i_1) \bullet \dots \bullet \pi_\gamma(x_1, \dots, x_n^{(1 \dots k)}, x_{n+1}) & \text{if } x_1 = \dots = x_{n-1} = 1, x_n \neq k \\ (TG(n, (1 \dots k)^{-1}, 1) \oplus i_1) \bullet \dots \bullet \pi_\gamma(x_1, \dots, x_n, x_{n+1}^{(12)}) & \text{if some } x_1, \dots, x_{n-1} \neq 1, x_n = 1 \\ (TG(n, (1 \dots k)^{-1}, 1) \oplus i_1) \bullet \dots \bullet \pi_\gamma(x_1, \dots, x_n, x_{n+1}) & \text{if some } x_1, \dots, x_{n-1} \neq 1, x_n \neq 1 \end{cases} \\
&= \begin{cases} (TG(n, (1 \dots k)^{-1}, 1) \oplus i_1) \bullet \dots \bullet (TG(n, (12), 1) \oplus i_1)(x_1, \dots, x_{n-1}, x_{n+1}^{(12)}, x_n^{(1 \dots k)}) & \text{if } x_1 = \dots = x_{n-1} = 1, x_n = k \\ (TG(n, (1 \dots k)^{-1}, 1) \oplus i_1) \bullet \dots \bullet (TG(n, (12), 1) \oplus i_1)(x_1, \dots, x_{n-1}, x_{n+1}, x_n^{(1 \dots k)}) & \text{if } x_1 = \dots = x_{n-1} = 1, x_n \neq k \\ (TG(n, (1 \dots k)^{-1}, 1) \oplus i_1) \bullet \dots \bullet (TG(n, (12), 1) \oplus i_1)(x_1, \dots, x_{n-1}, x_{n+1}^{(12)}, x_n) & \text{if some } x_1, \dots, x_{n-1} \neq 1, x_n = 1 \\ (TG(n, (1 \dots k)^{-1}, 1) \oplus i_1) \bullet \dots \bullet (TG(n, (12), 1) \oplus i_1)(x_1, \dots, x_{n-1}, x_{n+1}, x_n) & \text{if some } x_1, \dots, x_{n-1} \neq 1, x_n \neq 1 \end{cases}
\end{aligned}$$

$$\begin{aligned}
&= \left\{ \begin{array}{ll} (TG(n, (1 \dots k)^{-1}, 1) \oplus i_1) \bullet & \pi_\gamma(x_1, \dots, x_{n-1}, x_{n+1}^{(12)(12)}, x_n^{(1 \dots k)}) \\ & \text{if } x_1 = \dots = x_{n-1} = 1, x_n = k \\ (TG(n, (1 \dots k)^{-1}, 1) \oplus i_1) \bullet & \pi_\gamma(x_1, \dots, x_{n-1}, x_{n+1}^{(12)}, x_n^{(1 \dots k)}) \\ & \text{if } x_1 = \dots = x_{n-1} = 1, x_n \neq k \\ (TG(n, (1 \dots k)^{-1}, 1) \oplus i_1) \bullet & \pi_\gamma(x_1, \dots, x_{n-1}, x_{n+1}^{(12)}, x_n) \\ & \text{if some } x_1, \dots, x_{n-1} \neq 1, x_n = 1 \\ (TG(n, (1 \dots k)^{-1}, 1) \oplus i_1) \bullet & \pi_\gamma(x_1, \dots, x_{n-1}, x_{n+1}, x_n) \\ & \text{if some } x_1, \dots, x_{n-1} \neq 1, x_n \neq 1 \end{array} \right. \\
&= \left\{ \begin{array}{ll} (TG(n, (1 \dots k)^{-1}, 1) \oplus i_1) & (x_1, \dots, x_{n-1}, x_n^{(1 \dots k)}, x_{n+1}) \\ & \text{if } x_1 = \dots = x_{n-1} = 1, x_n = k \\ (TG(n, (1 \dots k)^{-1}, 1) \oplus i_1) & (x_1, \dots, x_{n-1}, x_n^{(1 \dots k)}, x_{n+1}^{(12)}) \\ & \text{if } x_1 = \dots = x_{n-1} = 1, x_n \neq k \\ (TG(n, (1 \dots k)^{-1}, 1) \oplus i_1) & (x_1, \dots, x_{n-1}, x_n, x_{n+1}^{(12)}) \\ & \text{if some } x_1, \dots, x_{n-1} \neq 1, x_n = 1 \\ (TG(n, (1 \dots k)^{-1}, 1) \oplus i_1) & (x_1, \dots, x_{n-1}, x_n, x_{n+1}) \\ & \text{if some } x_1, \dots, x_{n-1} \neq 1, x_n \neq 1 \end{array} \right. \\
&= \left\{ \begin{array}{ll} (x_1, \dots, x_{n-1}, x_n, x_{n+1}) & \text{if } x_1 = \dots = x_{n-1} = 1, x_n = k \\ (x_1, \dots, x_{n-1}, x_n, x_{n+1}^{(12)}) & \text{if } x_1 = \dots = x_{n-1} = 1, x_n \neq k \\ (x_1, \dots, x_{n-1}, x_n, x_{n+1}^{(12)}) & \text{if some } x_1, \dots, x_{n-1} \neq 1, x_n = 1 \\ (x_1, \dots, x_{n-1}, x_n, x_{n+1}) & \text{if some } x_1, \dots, x_{n-1} \neq 1, x_n \neq 1 \end{array} \right.
\end{aligned}$$

We see that Σ_1 is nonidentity iff:

1. Not all of x_1, \dots, x_{n-1} are 1 and $x_n = 1$, then $x_{n+1} \mapsto x_{n+1}^{(12)}$, or
2. $x_1 = \dots = x_{n-1} = 1$ and $x_n \neq k$, then $x_{n+1} \mapsto x_{n+1}^{(12)}$

For $m \in \{2, \dots, k-1\}$, let

$$\sigma_m = (TG(n, (1m), 1) \oplus i_1) \bullet (i_{n-1} \oplus TG(2, (12), 1)) \bullet (TG(n, (1m), 1) \oplus i_1)$$

We calculate

$$\begin{aligned}
& \sigma_m(x_1, \dots, x_{n+1}) \\
&= \begin{cases} (TG(n, (1m), 1) \oplus i_1) \bullet (i_{n-1} \oplus TG(2, (12), 1))(x_1, \dots, x_n^{(1m)}, x_{n+1}) & \text{if } x_1 = \dots = x_{n-1} = 1 \\ (TG(n, (1m), 1) \oplus i_1) \bullet (i_{n-1} \oplus TG(2, (12), 1))(x_1, \dots, x_n, x_{n+1}) & \text{if some } x_1, \dots, x_{n-1} \neq 1 \end{cases} \\
&= \begin{cases} (TG(n, (1m), 1) \oplus i_1)(x_1, \dots, x_n^{(1m)}, x_{n+1}^{(12)}) & \text{if } x_1 = \dots = x_{n-1} = 1, x_n = m \\ (TG(n, (1m), 1) \oplus i_1)(x_1, \dots, x_n^{(1m)}, x_{n+1}) & \text{if } x_1 = \dots = x_{n-1} = 1, x_n \neq m \\ (TG(n, (1m), 1) \oplus i_1)(x_1, \dots, x_n, x_{n+1}^{(12)}) & \text{if some } x_1, \dots, x_{n-1} \neq 1, x_n = 1 \\ (TG(n, (1m), 1) \oplus i_1)(x_1, \dots, x_n, x_{n+1}) & \text{if some } x_1, \dots, x_{n-1} \neq 1, x_n \neq 1 \end{cases} \\
&= \begin{cases} (x_1, \dots, x_n, x_{n+1}^{(12)}) & \text{if } x_1 = \dots = x_{n-1} = 1, x_n = m \\ (x_1, \dots, x_n, x_{n+1}) & \text{if } x_1 = \dots = x_{n-1} = 1, x_n \neq m \\ (x_1, \dots, x_n, x_{n+1}^{(12)}) & \text{if some } x_1, \dots, x_{n-1} \neq 1, x_n = 1 \\ (x_1, \dots, x_n, x_{n+1}) & \text{if some } x_1, \dots, x_{n-1} \neq 1, x_n \neq 1 \end{cases}
\end{aligned}$$

Once again this function is almost always identity, σ_m is nonidentity iff:

1. Not all of x_1, \dots, x_{n-1} are 1 and $x_n = 1$, then $x_{n+1} \mapsto x_{n+1}^{(12)}$, or
2. $x_1 = \dots = x_{n-1} = 1$ and $x_n = m$, then $x_{n+1} \mapsto x_{n+1}^{(12)}$.

Then define

$$\Sigma_2 = \sigma_{k-1} \bullet \dots \bullet \sigma_2$$

We have then that Σ_2 is nonidentity iff

1. Not all of x_1, \dots, x_{n-1} are 1 and $x_n = 1$, then $x_{n+1} \mapsto x_{n+1}^{(12)^{k-2}} = x_{n+1}^{(12)}$ because k and thus $k-2$ are odd, or
2. $x_1 = \dots = x_{n-1} = 1$ and $x_n \in \{2, \dots, k-1\}$, then $x_{n+1} \mapsto x_{n+1}^{(12)}$.

We see that $\Sigma_2 \bullet \Sigma_1$ is identity unless one of the factors is nonidentity. There are three cases:

1. Both are nonidentity by their first case. Then not all of x_1, \dots, x_{n-1} are 1 and $x_n = 1$, so

$$\begin{aligned}\Sigma_2 \bullet \Sigma_1(x_1 \dots x_{n+1}) &= \Sigma_2(x_1, \dots, x_{n+1}^{(12)}) \\ &= (x_1, \dots, x_{n+1}^{(12)(12)}) \\ &= (x_1, \dots, x_{n+1})\end{aligned}$$

so $\Sigma_2 \bullet \Sigma_1$ is the identity.

2. Both are nonidentity by their second case, so $x_1 = \dots = x_{n-1} = 1$ and $x_n \in \{2, \dots, k-1\}$,

$$\begin{aligned}\Sigma_2 \bullet \Sigma_1(x_1 \dots x_{n+1}) &= \Sigma_2(x_1, \dots, x_{n+1}^{(12)}) \\ &= (x_1, \dots, x_{n+1}^{(12)(12)}) \\ &= (x_1, \dots, x_{n+1})\end{aligned}$$

so $\Sigma_2 \bullet \Sigma_1$ is the identity.

3. Only Σ_1 is nonidentity by the second case, so $x_1 = \dots = x_n = 1$, then

$$\begin{aligned}\Sigma_2 \bullet \Sigma_1(x_1 \dots x_{n+1}) &= \Sigma_2(x_1, \dots, x_{n+1}^{(12)}) \\ &= (x_1, \dots, x_{n+1}^{(12)}) \\ &= (x_1, \dots, x_{n+1}^{(12)})\end{aligned}$$

so we have the only case that $\Sigma_2 \bullet \Sigma_1$ is nonidentity.

Thus we see that $\Sigma_2 \bullet \Sigma_1 = TG(n+1, (12), 1)$.

We now look at $TG(n+1, (1 \dots k), 1)$. Because the group generated by $(1 \dots k)$ is cyclic of odd order, the homomorphism $x \mapsto x^2$ of this group is an automorphism. Thus there exists some β such that $\beta^2 = (1 \dots k)$. This will also be a k -cycle, write $\beta = (\beta_1 \dots \beta_k)$. Let $k = 2l + 1$. Define $\alpha = (\beta_1 \beta_k)(\beta_2 \beta_{k-1}) \dots (\beta_l \beta_{l+2})$. Then $\alpha \beta \alpha = \beta^{-1}$, so $\beta \alpha \beta^{-1} \alpha = \beta^2 = (1 \dots k)$.

Let $\gamma = (n \ n+1)$ as a permutation on $\{1, \dots, n+1\}$. Now define

$$\begin{aligned}\Sigma &= \pi_\gamma \bullet (TG(n, \alpha, 1) \oplus i_1) \bullet \pi_\gamma \bullet (i_{n-1} \oplus TG(2, \beta^{-1}, 1)) \bullet \pi_\gamma \\ &\quad \bullet (TG(n, \alpha, 1) \oplus i_1) \bullet \pi_\gamma \bullet (i_{n-1} \oplus TG(2, \beta, 1))\end{aligned}$$

We calculate.

$$\begin{aligned}
& \Sigma(x_1, \dots, x_{n+1}) \\
&= \begin{cases} \pi_\gamma \bullet \dots \bullet \pi_\gamma(x_1, \dots, x_n, x_{n+1}^\beta) & x_n = 1 \\ \pi_\gamma \bullet \dots \bullet \pi_\gamma(x_1, \dots, x_n, x_{n+1}) & x_n \neq 1 \end{cases} \\
&= \begin{cases} \pi_\gamma \bullet \dots \bullet (TG(n, \alpha, 1) \oplus i_1)(x_1, \dots, x_{n+1}^\beta, x_n) & x_n = 1 \\ \pi_\gamma \bullet \dots \bullet (TG(n, \alpha, 1) \oplus i_1)(x_1, \dots, x_{n+1}, x_n) & x_n \neq 1 \end{cases} \\
&= \begin{cases} \pi_\gamma \bullet \dots \bullet \pi_\gamma(x_1, \dots, x_{n+1}^{\beta\alpha}, x_n) & x_1 = \dots = x_n = 1 \\ \pi_\gamma \bullet \dots \bullet \pi_\gamma(x_1, \dots, x_{n+1}^\beta, x_n) & \text{some } x_1, \dots, x_{n-1} \neq 1, x_n = 1 \\ \pi_\gamma \bullet \dots \bullet \pi_\gamma(x_1, \dots, x_{n+1}^\alpha, x_n) & x_1 = \dots = x_{n-1} = 1, x_n \neq 1 \\ \pi_\gamma \bullet \dots \bullet \pi_\gamma(x_1, \dots, x_{n+1}, x_n) & \text{some } x_1, \dots, x_{n-1} \neq 1, x_n \neq 1 \end{cases} \\
&= \begin{cases} \pi_\gamma \bullet \dots \bullet (i_{n-1} \oplus TG(2, \beta^{-1}, 1)) & (x_1, \dots, x_n, x_{n+1}^{\beta\alpha}) \\ & x_1 = \dots = x_n = 1 \\ \pi_\gamma \bullet \dots \bullet (i_{n-1} \oplus TG(2, \beta^{-1}, 1)) & (x_1, \dots, x_n, x_{n+1}^\beta) \\ & \text{some } x_1, \dots, x_{n-1} \neq 1, x_n = 1 \\ \pi_\gamma \bullet \dots \bullet (i_{n-1} \oplus TG(2, \beta^{-1}, 1)) & (x_1, \dots, x_n, x_{n+1}^\alpha) \\ & x_1 = \dots = x_{n-1} = 1, x_n \neq 1 \\ \pi_\gamma \bullet \dots \bullet (i_{n-1} \oplus TG(2, \beta^{-1}, 1)) & (x_1, \dots, x_n, x_{n+1}) \\ & \text{some } x_1, \dots, x_{n-1} \neq 1, x_n \neq 1 \end{cases} \\
&= \begin{cases} \pi_\gamma \bullet \dots \bullet \pi_\gamma(x_1, \dots, x_n, x_{n+1}^{\beta\alpha\beta^{-1}}) & x_1 = \dots = x_n = 1 \\ \pi_\gamma \bullet \dots \bullet \pi_\gamma(x_1, \dots, x_n, x_{n+1}^{\beta\beta^{-1}}) & \text{some } x_1, \dots, x_{n-1} \neq 1, x_n = 1 \\ \pi_\gamma \bullet \dots \bullet \pi_\gamma(x_1, \dots, x_n, x_{n+1}^\alpha) & x_1 = \dots = x_{n-1} = 1, x_n \neq 1 \\ \pi_\gamma \bullet \dots \bullet \pi_\gamma(x_1, \dots, x_n, x_{n+1}) & \text{some } x_1, \dots, x_{n-1} \neq 1, x_n \neq 1 \end{cases} \\
&= \begin{cases} \pi_\gamma \bullet (TG(n, \alpha, 1) \oplus i_1)(x_1, \dots, x_{n+1}^{\beta\alpha\beta^{-1}}, x_n) & x_1 = \dots = x_n = 1 \\ \pi_\gamma \bullet (TG(n, \alpha, 1) \oplus i_1)(x_1, \dots, x_{n+1}, x_n) & \text{some } x_1, \dots, x_{n-1} \neq 1, x_n = 1 \\ \pi_\gamma \bullet (TG(n, \alpha, 1) \oplus i_1)(x_1, \dots, x_{n+1}^\alpha, x_n) & x_1 = \dots = x_{n-1} = 1, x_n \neq 1 \\ \pi_\gamma \bullet (TG(n, \alpha, 1) \oplus i_1)(x_1, \dots, x_{n+1}, x_n) & \text{some } x_1, \dots, x_{n-1} \neq 1, x_n \neq 1 \end{cases} \\
&= \begin{cases} \pi_\gamma(x_1, \dots, x_{n+1}^{\beta\alpha\beta^{-1}\alpha}, x_n) & x_1 = \dots = x_n = 1 \\ \pi_\gamma(x_1, \dots, x_{n+1}, x_n) & \text{some } x_1, \dots, x_{n-1} \neq 1, x_n = 1 \\ \pi_\gamma(x_1, \dots, x_{n+1}^\alpha, x_n) & x_1 = \dots = x_{n-1} = 1, x_n \neq 1 \\ \pi_\gamma(x_1, \dots, x_{n+1}, x_n) & \text{some } x_1, \dots, x_{n-1} \neq 1, x_n \neq 1 \end{cases} \\
&= \begin{cases} (x_1, \dots, x_n, x_{n+1}^{\beta\alpha\beta^{-1}\alpha}) & x_1 = \dots = x_n = 1 \\ (x_1, \dots, x_n, x_{n+1}) & \text{some } x_1, \dots, x_{n-1} \neq 1, x_n = 1 \\ (x_1, \dots, x_n, x_{n+1}) & x_1 = \dots = x_{n-1} = 1, x_n \neq 1 \\ (x_1, \dots, x_n, x_{n+1}) & \text{some } x_1, \dots, x_{n-1} \neq 1, x_n \neq 1 \end{cases}
\end{aligned}$$

$$= \begin{cases} (x_1, \dots, x_n, x_{n+1}^{(1\dots k)}) & x_1 = \dots = x_n = 1 \\ (x_1, \dots, x_n, x_{n+1}) & \text{otherwise} \end{cases}$$

Thus we see that $\Sigma = TG(n+1, (1, \dots, k), 1)$.

We have shown that we can realise the two Toffoli gates that generate all of $\{TG(n+1, \alpha, o) | \alpha \in S_A\}$. Thus by Corollary 5.5, $B_{n+1}(A)$ is realised for all n , so by induction, all of $B(A)$ is realised. \square

Thus we have a small generating set for the bijections.

Corollary 5.11 *Let A be of odd order k . Let $\alpha = (1 \dots k), \beta = (12) \in S_A$. Then $B(A)$ is realised by $\{\alpha, \beta, TG(2, \alpha, 1), TG(2, \beta, 1)\}$.*

We see that when A is of odd order, $TG(i+1, \alpha, 1)$ is in the revclone generated by $\{TG(i, \alpha, 1) | \alpha \in S_A\}$, which is not the case for even order A . We see a distinct property looking at closure with temporary storage in the following. Note that $TG(n, \alpha, o) = s((2, 3, \dots, n+1), k(1, o, TG(n+1, \alpha, o))$ so $TG(n, \alpha, o)$ is realised with strong temporary storage from $TG(n+1, \alpha, o)$. We see that closure under T_S is a stronger form of generation.

Theorem 5.12 ([12] Thm 5.3) *Let A be a set, $o \in A$. For every n , for every $\alpha, TG(n, \alpha, o)$ can be realised with strong temporary storage by $\{TG(i, \alpha, o) | i \leq 3, \alpha \in S_A\}$.*

Proof: We proceed by induction. Assume that we can construct $TG(n-1, \alpha, o)$ for all α . Let $p \in A$ some non- o element, $\beta = (op)$ be an involution of A . Define $f \in B_{n+1}(A)$ by

$$f = (TG(n-1, \beta, o) \oplus i_2) \bullet (i_{n-2} \oplus TG(3, \alpha, o)) \bullet (TG(n-1, \beta, o) \oplus i_2)$$

Then

$$\begin{aligned} & f(x_1, \dots, x_{n+1}) \\ &= \begin{cases} (TG(n-1, \beta, o) \oplus i_2) \bullet (i_{n-2} \oplus TG(3, \alpha, o))(x_1, \dots, x_{n-1}^\beta, x_n, x_{n+1}) & x_1 = \dots = x_{n-2} = o \\ (TG(n-1, \beta, o) \oplus i_2) \bullet (i_{n-2} \oplus TG(3, \alpha, o))(x_1, \dots, x_{n-1}, x_n, x_{n+1}) & \text{otherwise} \end{cases} \end{aligned}$$

$$\begin{aligned}
&= \begin{cases} (TG(n-1, \beta, o) \oplus i_2)(x_1, \dots, x_{n-1}^\beta, x_n, x_{n+1}^\alpha) \\ \quad x_1 = \dots = x_{n-2} = x_{n-1}^\beta = x_n = o \\ (TG(n-1, \beta, o) \oplus i_2)(x_1, \dots, x_{n-1}^\beta, x_n, x_{n+1}) \\ \quad x_1 = \dots = x_{n-2} = o \wedge (x_{n-1}^\beta \neq o \vee x_n \neq o) \\ (TG(n-1, \beta, o) \oplus i_2)(x_1, \dots, x_{n-1}, x_n, x_{n+1}^\alpha) \\ \quad x_j \neq o \exists j \leq n-2, x_{n-1} = x_n = o \\ (TG(n-1, \beta, o) \oplus i_2)(x_1, \dots, x_{n-1}, x_n, x_{n+1}) \quad \text{otherwise} \end{cases} \\
&= \begin{cases} (x_1, \dots, x_{n-1}, x_n, x_{n+1}^\alpha) & x_1 = \dots = x_{n-2} = x_{n-1}^\beta = x_n = o \\ (x_1, \dots, x_{n-1}, x_n, x_{n+1}) & x_1 = \dots = x_{n-2} = o \wedge \\ & (x_{n-1}^\beta \neq o \vee x_n \neq o) \\ (x_1, \dots, x_{n-1}, x_n, x_{n+1}^\alpha) & x_j \neq o \exists j \leq n-2, x_{n-1} = x_n = o \\ (x_1, \dots, x_{n-1}, x_n, x_{n+1}) & \text{otherwise} \end{cases}
\end{aligned}$$

Note that $f_i(x_1, \dots, x_{n+1}) = x_i$ for all $i \leq n$.

Let g be the reduct

$$g(x_1, \dots, x_n) = s((1, 2, \dots, n-2, n, n+1), k(n-1, p, f))$$

From above we obtain, knowing that $p^\beta = o$ and $p \neq o$

$$\begin{aligned}
&k(n-1, p, f)(x_1, \dots, x_n) \\
&= f(x_1, \dots, x_{n-2}, p, x_{n-1}, x_n) \\
&= \begin{cases} (x_1, \dots, x_{n-2}, p, x_{n-1}, x_n^\alpha) & x_1 = \dots = x_{n-2} = p^\beta = x_{n-1} = o \\ (x_1, \dots, x_{n-2}, p, x_{n-1}, x_n) & x_1 = \dots = x_{n-2} = o \wedge \\ & (p^\beta \neq o \vee x_{n-1} \neq o) \\ (x_1, \dots, x_{n-2}, p, x_{n-1}, x_n^\alpha) & x_j \neq o \exists j \leq n-2, \\ & p = x_{n-1} = o \text{ [contradiction]} \\ (x_1, \dots, x_{n-2}, p, x_{n-1}, x_n) & \text{otherwise} \end{cases} \\
&= \begin{cases} (x_1, \dots, x_{n-2}, p, x_{n-1}, x_n^\alpha) & x_1 = \dots = x_{n-2} = x_{n-1} = o \\ (x_1, \dots, x_{n-2}, p, x_{n-1}, x_n) & x_1 = \dots = x_{n-2} = o \wedge (x_{n-1} \neq o) \\ (x_1, \dots, x_{n-2}, p, x_{n-1}, x_n) & \text{otherwise} \end{cases} \\
&= \begin{cases} (x_1, \dots, x_{n-2}, p, x_{n-1}, x_n^\alpha) & x_1 = \dots = x_{n-2} = x_{n-1} = o \\ (x_1, \dots, x_{n-2}, p, x_{n-1}, x_n) & \text{otherwise} \end{cases}
\end{aligned}$$

Thus

$$\begin{aligned}
g(x_1, \dots, x_n) &= s((1, 2, \dots, n-2, n, n+1), k(n-1, p, f))(x_1, \dots, x_n) \\
&= \begin{cases} (x_1, \dots, x_{n-2}, x_{n-1}, x_n^\alpha) & x_1 = \dots = x_{n-2} = x_{n-1} = o \\ (x_1, \dots, x_{n-2}, x_{n-1}, x_n) & \text{otherwise} \end{cases} \\
&= TG(n, \alpha, o)
\end{aligned}$$

Note that $g_{n-1}(x_1, \dots, x_{n+1}) = x_{n-1}$, a trivial permutation, so we have strong temporary storage. \square

Thus we see some essential differences between isomorphic realisation and realisation with (strong) temporary storage. In the next section we will further investigate the differences between certain types of realisation and closure.

6 VARIOUS CLOSURES

The following result shows us how the various class and closure operators that we have seen above relate and thus we will be able to determine a lot of information about the relationships between various types of closure.

Theorem 6.1 $KK = K$, $SS = S$, $CC = C$, $C_\Delta C_\Delta = C_\Delta$, $SC = CS$, $KC = CK$, $C_\Delta K = KC_\Delta$, $C_\Delta S = SC_\Delta$ and $SK = KS$.

Proof: The K and S operators are idempotent as a simple implication of the definitions. The C and C_Δ operators are idempotent because they are algebraic closure operations.

To show that $SC = CS$ we show that all multicloning operations commute with s . We use the operation set $\{\oplus, \pi_\alpha, \circ_k | \alpha \in S_A, k \in \mathbb{N}\}$. We start with the inclusion $SC \subseteq CS$. Let $f \in M_{n,m}(A)$, $g \in M_{l,p}(A)$, $r \in \mathbb{N}$, $I \in \{1, \dots, m+p\}^r$, $\alpha \in S_m$.

Let $J \subseteq \{1, \dots, r\}$ such that $j \in J$ iff $I_j \leq m$. Write $J = \{j_1, \dots, j_t\}$. Then let $I' = (I_{j_i} | i \in (1, \dots, t)) \in \{1, \dots, m\}^t$. Let $\{1, \dots, r\} \setminus J = \{\bar{j}_1, \dots, \bar{j}_u\}$. Then let $I'' = (I_{\bar{j}_i} - m | i \in (1, \dots, u)) \in \{1, \dots, p\}^u$. Finally define $\beta \in S_r$ with

$$\beta : i \mapsto h \text{ such that } \begin{cases} h = j_i & i \leq t \\ h = \bar{j}_{i-t} & i > t \end{cases}$$

which can be written as

$$\beta = \begin{pmatrix} 1 & \dots & t & t+1 & \dots & r \\ j_1 & \dots & j_t & \bar{j}_1 & \dots & \bar{j}_u \end{pmatrix}$$

Note that $i \leq t$ iff $I_{\beta(i)} \leq m$ and that $I_i = I'_{\beta^{-1}i}$ if $I_i \leq m$, $I_i = I''_{(\beta^{-1}i)-t} + m$ otherwise. Then we claim that

$$s(I, f \oplus g) = \pi_\beta(s(I', f) \oplus s(I'', g))$$

The left hand side is

$$s(I, f \oplus g)_i = \begin{cases} (f)_{I_i} & I_i \leq m \\ (g)_{I_i-m} & I_i > m \end{cases}$$

The right hand side is

$$\begin{aligned} \pi_\beta(s(I', f) \oplus s(I'', g))_i &= (s(I', f) \oplus s(I'', g))_{\beta^{-1}i} \\ &= \begin{cases} s(I', f)_{\beta^{-1}i} & \beta^{-1}i \leq t \\ s(I'', g)_{(\beta^{-1}i)-t} & \beta^{-1}i > t \end{cases} \\ &= \begin{cases} (f)_{I'_{\beta^{-1}i}} & \beta^{-1}i \leq t \\ (g)_{I''_{(\beta^{-1}i)-t}} & \beta^{-1}i > t \end{cases} \\ &= \begin{cases} (f)_{I_i} & I_i \leq m \\ (g)_{I_i-m} & I_i > m \end{cases} \end{aligned}$$

which shows our claim.

It is a simple calculation that

$$s(I, \pi_\alpha f) = s(\alpha^{-1}(I), f)$$

where α^{-1} acts upon the entries in I , so $(\alpha^{-1}I)_i = \alpha^{-1}(I_i)$.

For composition, we use a similar argument to the \oplus case above. Assume that I is increasing. Let $I' = (I_1, \dots, I_t)$ with $I_t \leq m$, $I_{t+1} > m$. Let $I'' = (1, \dots, k) \oplus (I_{t+1} - m + k, \dots, I_r - m + k)$. We claim that

$$s(I, f \circ_k g) = s(I', f) \circ_k s(I'', g)$$

The left hand side is

$$s(I, f \circ_k g)_i = \begin{cases} f_{I_i} \circ_k g & i \leq t \\ g_{I_i-m+k} & i > t \end{cases}$$

The right hand side is

$$\begin{aligned}
(s(I', f) \circ_k s(I'', g))_i &= \begin{cases} s(I', f)_i \circ_k s(I'', g) & i \leq t \\ s(I'', g)_{i-t+k} & i > t \end{cases} \\
&= \begin{cases} f_{I'_i} \circ_k g & i \leq t \text{ because of the first } k \text{ entries in } I'' \\ g_{I''_{i-t+k}} & i > t \end{cases} \\
&= \begin{cases} f_{I_i} \circ_k g & i \leq t \\ g_{I_i-m+k} & i > t \end{cases}
\end{aligned}$$

Which is what we wanted. If I is not increasing, then there is a permutation $\beta \in S_r$ such that $\pi_\beta I$ is increasing. Then

$$s(I, f \circ_k g) = \pi_{\beta^{-1}} s(\pi_\beta I, f \circ_k g) = \pi_{\beta^{-1}} (s(I', f) \circ_k s(I'', g))$$

Thus we see that $SC \subseteq CS$.

For the converse, i.e. $CS \subseteq SC$, we use similar techniques. Let $f \in M_{n,m}(A)$, $g \in M_{l,p}(A)$, $t, u \in \mathbb{N}$, $I' \in \{1, \dots, m\}^t$, $I'' \in \{1, \dots, p\}^u$, $\alpha \in S_t$.

Let $I = I' \oplus (I'' + m)$, i.e. $I_i = I'_i$ for $i \leq t$, $I_i = I''_{i-t} + m$ for $i > t$. Then it is a simple calculation to see that

$$s(I', f) \oplus s(I'', g) = s(I, f \oplus g)$$

Let $I \in \{1, \dots, m\}^t$, define $I_i^\alpha = I_{\alpha^{-1}i}$. Then we see that

$$\pi_\alpha s(I, f) = s(I^\alpha, f)$$

Let $\beta \in S_p$ be defined by $\beta^{-1}(i) = I''_i$ for $i \leq u$, with the rest filled in to make it a permutation. Because I'' contains no repeats, we know this can be done. Let $k \leq \min(n, u)$. Then we claim that

$$s(I', f) \circ_k s(I'', g) = s(I' \oplus (m+1, \dots, m+u-k), f \circ_k (\pi_\beta \circ_p g))$$

For $i \leq t$ we have

$$\begin{aligned}
&(s(I', f) \circ_k s(I'', g))_i(x_1, \dots, x_{l+n-k}) \\
&= f_{I'_i} \circ_k s(I'', g)(x_1, \dots, x_{l+n-k}) \\
&= f_{I'_i}(g_{I''_1}(x_1, \dots, x_l), \dots, g_{I''_k}(x_1, \dots, x_l), x_{l+1}, \dots, x_{l+n-k}) \\
&= f_{I'_i}(g_{\beta^{-1}1}(x_1, \dots, x_l), \dots, g_{\beta^{-1}k}(x_1, \dots, x_l), x_{l+1}, \dots, x_{l+n-k}) \\
&= (s(I' \oplus (m+1, \dots, m+u-k), f \circ_k (\pi_\beta \circ_p g)))_i(x_1, \dots, x_{l+n-k})
\end{aligned}$$

while for $t < i \leq m + u - k$ we have

$$\begin{aligned}
& (s(I', f) \circ_k s(I'', g))_i(x_1, \dots, x_{l+n-k}) \\
&= g_{I''_{k+i-t}}(x_1, \dots, x_l) \\
&= g_{\beta^{-1}(k+i-t)}(x_1, \dots, x_l) \\
&= (\pi_\beta \circ_p g)_{k+(i-t)}(x_1, \dots, x_l) \\
&= (f \circ_k (\pi_\beta \circ_p g))_{m+i-t}(x_1, \dots, x_{l+n-k}) \\
&= s(I' \oplus (m+1, \dots, m+u-k), f \circ_k (\pi_\beta \circ_p g))_i(x_1, \dots, x_{l+n-k})
\end{aligned}$$

Thus we have that $CS \subseteq SC$ and thus $SC = CS$.

Similarly we show that $KC = CK$. We start with $KC \subseteq CK$. Let $f \in M_{n,m}(A)$, $g \in M_{l,p}(A)$, $i \in \{1, \dots, n+l\}$, $a \in A$. It is a simple application of the definitions to see that

$$k(i, a, f \oplus g) = \begin{cases} k(i, a, f) \oplus g & i \leq n \\ f \oplus k(i-n, a, g) & i > n \end{cases}$$

Let $f \in M_{n,m}(A)$, $\alpha \in S_m$, $i \in \{1, \dots, n\}$, $a \in A$. It is a simple calculation that

$$k(i, a, \pi_\alpha f) = \pi_\alpha k(i, a, f)$$

Let $f \in M_{n,m}(A)$, $g \in M_{l,p}(A)$, $k \leq \min(n, p)$, $i \in \{1, \dots, n+l\}$, $a \in A$. Applying the definitions gives us

$$k(i, a, f \circ_k g) = \begin{cases} f \circ_k k(i, a, g) & i \leq n \\ k(i+k-n, a, f) \circ_k g & i > n \end{cases}$$

For $CK \subseteq KC$ we proceed as follows. Note that we must also include the nonapplication of k as a case here. Let $f \in M_{n,m}(A)$, $g \in M_{l,p}(A)$, $i_1 \in \{1, \dots, n\}$, $i_2 \in \{1, \dots, l\}$, $a_1, a_2 \in A$. Then we claim that

$$\begin{aligned}
k(i_1, a_1, f) \oplus g &= k(i_1, a_1, f \oplus g) \\
f \oplus k(i_2, a_2, g) &= k(i_2 + n, a_2, f \oplus g) \\
k(i_1, a_1, f) \oplus k(i_2, a_2, g) &= k(i_1, a_1, k(i_2 + n, a_2, f \oplus g))
\end{aligned}$$

The first two follow by simple application of the definitions. The third claim combines these two.

As we saw above, π_α commutes with k .

Let $f \in M_{n,m}(A)$, $g \in M_{l,p}(A)$, $k \leq \min(n, p)$, $i_1 \in \{1, \dots, n\}$, $i_2 \in \{1, \dots, l\}$, $a_1, a_2 \in A$. Let $\beta \in S_n$ be $(i_1, i_1 + 1, \dots, n)$. Then we claim that

$$\begin{aligned} f \circ_k k(i_2, a_2, g) &= k(i_2, a_2, f \circ_k g) \\ k(i_1, a_1, f) \circ_k g &= \begin{cases} k(l + n - k, a_1, (f \circ_n \pi_\beta) \circ_k g) & i_1 \leq k \\ k(i_1 + l - k, a_1, f \circ_k g) & i_1 > k \end{cases} \\ k(i_1, a_1, f) \circ_k k(i_2, a_2, g) &= \begin{cases} k(i_2, a_2, k(l + n - k, a_1, (f \circ_n \pi_\beta) \circ_k g)) & i_1 \leq k \\ k(i_2, a_2, k(i_1 + l - k, a_1, f \circ_k g)) & i_1 > k \end{cases} \end{aligned}$$

The first claim is direct from the definitions. The second requires some more work. Let $i \in \{1, \dots, m + p - k\}$.

$$\begin{aligned} & (k(i_1, a_1, f) \circ_k g)_i(x_1, \dots, x_{n+l-k-1}) \\ &= \begin{cases} (k(i_1, a_1, f)_i \circ_k g)(x_1, \dots, x_{n+l-k-1}) & i \leq m \\ g_{i-m+k}(x_1, \dots, x_l) & i > m \end{cases} \\ &= \begin{cases} \begin{aligned} & f_i(g_1(x_1, \dots, x_l), \dots, g_{i_1-1}(\dots), a_1, g_{i_1}(\dots), \dots \\ & \dots, g_k(x_1, \dots, x_l), x_{l+1}, \dots, x_{n+l-k-1}) \end{aligned} & i_1 \leq k, i \leq m \\ \begin{aligned} & f_i(g_1(x_1, \dots, x_l), \dots, g_k(x_1, \dots, x_l), x_{l+1}, \dots \\ & \dots, x_{i_1-k+l-1}, a_1, x_{i_1+l-k}, \dots, x_{n+l-k-1}) \end{aligned} & i_1 > k, i \leq m \\ g_{i-m+k}(x_1, \dots, x_l) & i > m \end{cases} \\ &= \begin{cases} \begin{aligned} & (f \circ_n \pi_\beta)_i(g_1(x_1, \dots, x_l), \dots, g_{i_1-1}(\dots), g_{i_1}(\dots), \dots \\ & \dots, g_k(x_1, \dots, x_l), x_{l+1}, \dots, x_{n+l-k-1}, a_1) \end{aligned} & i_1 \leq k, i \leq m \\ k(i_1 + l - k, a_1, f \circ_k g)_i(x_1, \dots, x_{n+l-k-1}) & i_1 > k, i \leq m \\ g_{i-m+k}(x_1, \dots, x_l) & i > m \end{cases} \\ &= \begin{cases} k(l + n - k, a_1, (f \circ_n \pi_\beta) \circ_k g)_i(x_1, \dots, x_{n+l-k-1}) & i_1 \leq k, i \leq m \\ k(i_1 + l - k, a_1, f \circ_k g)_i(x_1, \dots, x_{n+l-k-1}) & i_1 > k, i \leq m \\ g_{i-m+k}(x_1, \dots, x_l) & i > m \end{cases} \\ &= \begin{cases} k(l + n - k, a_1, (f \circ_n \pi_\beta) \circ_k g)_i(x_1, \dots, x_{n+l-k-1}) & i_1 \leq k \\ k(i_1 + l - k, a_1, f \circ_k g)_i(x_1, \dots, x_{n+l-k-1}) & i_1 > k \end{cases} \end{aligned}$$

which is what we wanted. The third case is the combination of the first two cases.

So every expression in CK can be written in KC , so we obtain $CK = KC$.

We see that $SK = KS$ because it makes no difference whether the inputs are fed constants and then some outputs are ignored, or some outputs are ignored and then some inputs are fed constants. To see this formally, let $f \in M_{n,m}(A)$, $1 \leq i \leq n$, $r \in \mathbb{N}$, $I \in \{1, \dots, m\}^r$ and $a \in A$.

$$\begin{aligned} s(I, k(i, a, f))(x_1, \dots, x_{n-1}) &= s(I, f(x_1, \dots, x_{i-1}, a, x_i, \dots, x_{n-1})) \\ &= (f_j(x_1, \dots, x_{i-1}, a, x_i, \dots, x_{n-1}) | j \in I) \\ &= (k(i, a, f_j) | j \in I)(x_1, \dots, x_{n-1}) \\ &= k(i, a, s(I, f)) \end{aligned}$$

Lastly, we show that C_Δ is well behaved by showing that Δ and ∇ commute with S and K . Let $f \in M_{n,m}(A)$, $r \in \mathbb{N}$, $I \in \{1, \dots, n\}^r$ and $a \in A$.

$$\begin{aligned} s(I, \Delta f)(x_1, \dots, x_{n-1}) &= s(I, f(x_1, x_1, x_2, \dots, x_{n-1})) \\ &= (f_j(x_1, x_1, x_2, \dots, x_{n-1}) | j \in I) \\ &= \Delta(f_j(x_1, x_2, \dots, x_{n-1}) | j \in I) \\ &= \Delta s(I, f)(x_1, \dots, x_{n-1}) \\ s(I, \nabla f)(x_1, \dots, x_{n+1}) &= s(I, f(x_2, \dots, x_{n+1})) \\ &= (f_j(x_2, \dots, x_{n+1}) | j \in I) \\ &= \nabla s(I, f)(x_1, \dots, x_{n+1}) \end{aligned}$$

So we see that $C_\Delta S = SC_\Delta$.

Now let $f \in M_{n,m}(A)$, $1 \leq i \leq n$ and $a \in A$.

$$\begin{aligned} k(i, a, \Delta f)(x_1, \dots, x_{n-2}) &= (\Delta f)(x_1, \dots, x_{i-1}, a, x_i, \dots, x_{n-2}) \\ &= f(x_1, x_1, x_2, \dots, x_{i-1}, a, x_i, \dots, x_{n-2}) \\ &= \begin{cases} f(a, a, x_1, \dots, x_{n-2}) & i = 1 \\ f(x_1, x_1, a, x_2, \dots, x_{n-2}) & i = 2 \\ f(x_1, x_1, x_2, \dots, x_{i-1}, a, x_i, \dots, x_{n-2}) & i > 2 \end{cases} \\ &= \begin{cases} k(1, a, k(1, a, f)) & i = 1 \\ \Delta k(i+1, a, f) & i \geq 2 \end{cases} \end{aligned}$$

$$\begin{aligned}
k(i, a, \nabla f)(x_1, \dots, x_n) &= (\nabla f)(x_1, \dots, x_{i-1}, a, x_i, \dots, x_n) \\
&= \begin{cases} (\nabla f)(a, x_1, \dots, x_n) & i = 1 \\ (\nabla f)(x_1, x_2, \dots, x_{i-1}, a, x_i, \dots, x_n) & i > 1 \end{cases} \\
&= \begin{cases} f(x_1, \dots, x_n) & i = 1 \\ f(x_2, \dots, x_{i-1}, a, x_i, \dots, x_n) & i > 1 \end{cases} \\
&= \begin{cases} f(x_1, \dots, x_n) & i = 1 \\ \nabla k(i-1, a, f)(x_1, \dots, x_n) & i > 1 \end{cases}
\end{aligned}$$

Thus we have $KC_\Delta \subseteq C_\Delta K$. For the converse we calculate.

$$\begin{aligned}
&k(i, a, f)(x_1, \dots, x_{n-1}) \\
&= \begin{cases} f(a, x_1, x_2, \dots, x_{n-1}) & i = 1 \\ f(x_1, a, x_2, \dots, x_{n-1}) & i = 2 \\ f(x_1, x_2, \dots, x_{i-1}, a, x_i, \dots, x_{n-1}) & i > 2 \end{cases} \\
&\Rightarrow \Delta k(i, a, f)(x_1, \dots, x_{n-2}) \\
&= \begin{cases} f(a, x_1, x_1, x_2, \dots, x_{n-2}) & i = 1 \\ f(x_1, a, x_1, x_2, \dots, x_{n-2}) & i = 2 \\ f(x_1, x_1, x_2, \dots, x_{i-2}, a, x_{i-1}, \dots, x_{n-2}) & i > 2 \end{cases} \\
&= \begin{cases} k(2, a, \Delta(f \bullet \pi_{(1\ 2\ 3)}))(x_1, \dots, x_{n-2}) & i = 1 \\ k(2, a, \Delta(f \bullet \pi_{(2\ 3)}))(x_1, \dots, x_{n-2}) & i = 2 \\ k(i-1, a, \Delta f)(x_1, \dots, x_{n-2}) & i > 2 \end{cases} \\
&\nabla k(i, a, f)(x_1, \dots, x_n) \\
&= k(i, a, f)(x_2, \dots, x_n) \\
&= f(x_2, \dots, x_i, a, x_{i+1}, \dots, x_n) \\
&= (\nabla f)(x_1, \dots, x_i, a, x_{i+1}, \dots, x_n) \\
&= k(i+1, a, \nabla f)(x_1, \dots, x_n)
\end{aligned}$$

So we see that $KC_\Delta \subseteq C_\Delta K \subseteq KC_\Delta$ so they are equal. \square

Let $F \subseteq M(A)$ be a collection of mappings. Then $g \in SKC(F)$ is equivalent to saying that g is realised by F . We see that we have some inclusions amongst the various closure operations introduced above, obtaining the inclusion diagram in Figure 1.

We know that many of these inclusions are strict. For A of even order, we know from Corollary 5.8 and Theorem 5.12 that $C(F)$ is strictly included in

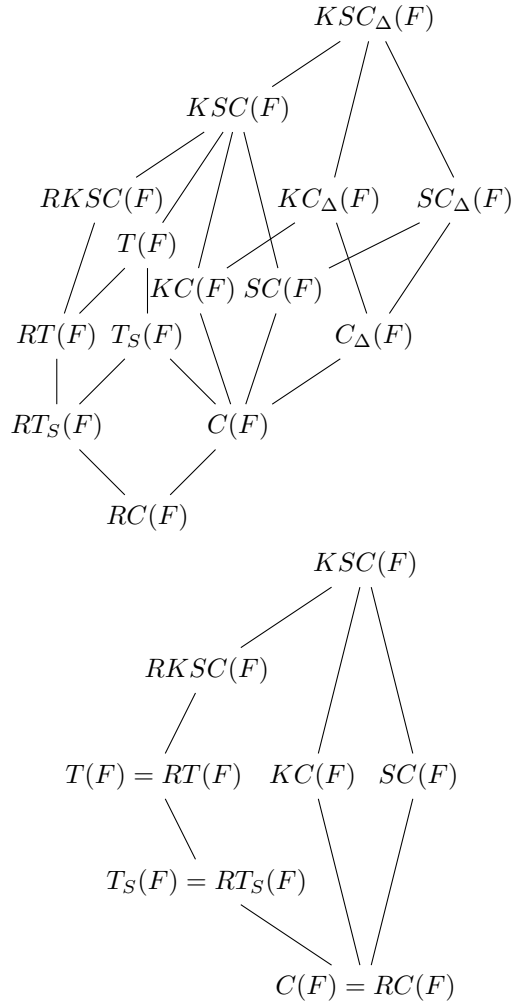


FIGURE 1

On the left we have inclusion of the various closure operations applied to a set of maps $F \subseteq M(A)$. When we are looking at a set $F \subseteq B(A)$ and are not interested in Δ , we get the inclusions on the right.

$T_S(F)$.

On the other hand, for specific classes of F , some closure classes fall together. If $F \subseteq B(A)$, then $RC(F) = C(F)$, $RT_S(F) = T_S(F)$ and $RT(F) = T(F)$. Thus we obtain the second inclusion diagram, where we also omit the Δ operator.

One of the general problems is to look at the ways in which we can define these various classes as a form of closure via a Galois connection. This has been preliminarily investigated in [6] for $C(F)$ and $T(F)$ from reversible F .

7 CONCLUSION

We have presented a language based upon clone theory in order to discuss systems of mappings $A^m \rightarrow A^n$ on a set A . We have then written Toffoli's model of reversible computation as a theory of mapping composition, finding that larger sets of states leads to a more complex system than binary reversible logic.

We see that the ideas can be used more generally. We are now confronted with the spectrum of questions that arise naturally in clone theory and related fields of general algebra, such as the size and structure of the lattice of multiclones and revclones on a given set. The largest challenge is to determine a suitable combinatorial structure to be used for invariance type results of the Pol-Inv type for the five natural types of closure. It seems probable that the results in [1, 6] will be of use to develop such a theory.

8 ACKNOWLEDGMENTS

I would like to thank Erhard Aichinger for many interesting conversations and suggestions about developing and presenting this paper.

REFERENCES

- [1] Scott Aaronson, Daniel Grier, and Luke Schaeffer. (2015). The classification of reversible bit operations. *Electronic Colloquium on Computational Complexity*, (66).
- [2] Stanley Burris and H. P. Sankappanavar. (1981). *A course in universal algebra*, volume 78 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin.
- [3] Miguel Couceiro and Erkkö Lehtonen. (2012). Galois theory for sets of operations closed under permutation, cylindrification, and composition. *Algebra Universalis*, 67(3):273–297.
- [4] The GAP Group. (2013). *GAP – Groups, Algorithms, and Programming, Version 4.6.5*.
- [5] N. Gershenfeld. (1996). Signal entropy and the thermodynamics of computation. *IBM Systems Journal*, 35(3 & 4).

- [6] Emil Jeřábek, (September 2014). Answer to classifying reversible gates. Theoretical Computer Science Stack Exchange. <http://cstheory.stackexchange.com/questions/25730>, Accessed June 2015.
- [7] Erko Lehtonen. (2010). Closed classes of functions, generalized constraints, and clusters. *Algebra Universalis*, 63(2-3):203–234.
- [8] A. I. Mal'tsev. (1976). *Iterativnye algebry Posta*. Novosibirsk. Gos. Univ., Novosibirsk. Seriya "Biblioteka Kafedry Algebry i Matematicheskoi Logiki Novosibirskogo Universiteta", Vyp. 16. ["Library of the Department of Algebra and Mathematical Logic of Novosibirsk State University" Series, No. 16].
- [9] Michael A. Nielsen and Isaac L. Chuang. (2000). *Quantum computation and quantum information*. Cambridge University Press, Cambridge.
- [10] R. Pöschel and L. A. Kalužnin. (1979). *Funktionen- und Relationenalgebren [Function and Relation algebras]*, volume 15 of *Mathematische Monographien [Mathematical Monographs]*. VEB Deutscher Verlag der Wissenschaften, Berlin. Ein Kapitel der diskreten Mathematik. [A chapter in discrete mathematics].
- [11] Ágnes Szendrei. (1986). *Clones in universal algebra*, volume 99 of *Séminaire de Mathématiques Supérieures [Seminar on Higher Mathematics]*. Presses de l'Université de Montréal, Montreal, QC.
- [12] Tommaso Toffoli. (1980). Reversible computing. Technical Report MIT/LCS/TM-151, MIT.
- [13] Tommaso Toffoli. (1980). Reversible computing. In *Automata, languages and programming (Proc. Seventh Internat. Colloq., Noordwijkerhout, 1980)*, volume 85 of *Lecture Notes in Comput. Sci.*, pages 632–644. Springer, Berlin-New York.
- [14] Guowu Yang, Xiaoyu Song, Marek Perkowski, and Jinzhao Wu. (2005). Realizing ternary quantum switching networks without ancilla bits. *J. Phys. A*, 38(44):9689–9697.